

Amendment to the Abstract

Please replace the entire abstract with the following amended abstract:

~~The invention concerns~~ A fast cryptographic method between two entities exchanging data via a non-secure communication channel. The method, for example, ~~for forming~~ forms a common key between two entities (A,B), each having a secret key (a,b) and using a public key (P) formed by a point of an elliptic curve (E), and includes ~~comprises~~ at least a ~~step which consists in~~ multiplying ~~said the~~ odd order point (P) by an integer ~~and said phase comprises operations called~~ by additions and halving operations. ~~the latter operation characterizing the invention.~~